

1
2 **CLAIMS:**

3 1. A computer-readable medium having computer-executable
4 instructions that, when executed by a computer, performs acts comprising:

5 obtaining two input polynomials each with degree ≤ 5 ;

6 computing a product polynomial of the input polynomials, wherein the total
7 number of coefficient multiplication operations is fewer than or equal to
8 seventeen;

9 reporting results of the computing.

10
11 2. A medium as recited in claim 1 further comprising repeating the
12 obtaining and the computing.

13
14 3. A medium as recited in claim 1 further comprising:

15 selecting a pair of polynomials from a collection of pairs and providing the
16 selected polynomials to the obtaining;

17 repeating the selecting, obtaining, and computing.
18
19
20
21
22
23
24
25

4. A medium as recited in claim 1, wherein during the computing, calculating:

$$\begin{aligned}
& (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
& + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
& + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
& + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - X^3) \\
& + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
& + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
& + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X^2) \\
& + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X^3) \\
& + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
& + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
& + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
& + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
& + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial, where C is a polynomial constant value and the two input polynomials are nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$, respectively.

1
2 5. A medium as recited in claim 4, wherein the variable X is replaced
3 by its negative ($-X$) and the odd-indexed coefficients, $a_1, a_3, a_5, b_1, b_3, b_5$, are
4 replaced by their negatives.

5
6 6. A medium as recited in claim 4, wherein the computing is performed
7 in a finite field of characteristic 2, with each even coefficient replaced by zero and
8 each odd coefficient replaced by one.

9
10 7. A medium as recited in claim 4, wherein the computing is performed
11 in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its
12 modulo 3 image 0, 1 or -1 .

13
14 8. A medium as recited in claim 1, wherein the two input polynomials
15 are representative of integers, which are nominally labeled: $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$
16 and $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$, respectively, where $0 \leq a_i < R$ and $0 \leq b_j < R$.

17
18 9. A medium as recited in claim 8, wherein j is ≥ 0 and ≤ 5 .

19
20 10. A computing device comprising:

21 an audio/visual output ;

22 a medium as recited in claim 1.
23
24
25

11. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining two input polynomials each with degree ≤ 5 ;

computing a product polynomial of the input polynomials, wherein such computing comprises calculating:

$$\begin{aligned}
& (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
& + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
& + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
& + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - X^3) \\
& + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
& + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
& + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X^2) \\
& + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X^3) \\
& + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
& + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
& + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
& + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
& + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

1 to compute the product polynomial, where C is an constant value and the two input
2 polynomials are nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 +$
3 a_5X^5 and $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$, respectively;
4 reporting results of the computing.

5
6 **12.** A medium as recited in claim 11, wherein the variable X is replaced
7 by its negative ($-X$) and the odd-indexed coefficients, $a_1, a_3, a_5, b_1, b_3, b_5$, are
8 replaced by their negatives.

9
10 **13.** A medium as recited in claim 11, wherein the computing is
11 performed in a finite field of characteristic 2, with each even coefficient replaced
12 by zero and each odd coefficient replaced by one.

13
14 **14.** A medium as recited in claim 11, wherein the computing is
15 performed in a finite field of characteristic 3, with each coefficient in claim 4
16 replaced by its modulo 3 image 0, 1 or -1 .

17
18 **15.** A medium as recited in claim 11 further comprising repeating the
19 obtaining and the computing.

20
21 **16.** A medium as recited in claim 11 further comprising:
22 selecting a pair of polynomials from a collection of one or more pairs of
23 polynomials and providing the selected polynomials to the obtaining;
24 repeating the selecting, obtaining, and computing.

1 17. A medium as recited in claim 11, wherein the total number of
2 coefficient multiplication operations performed during the computing is fewer
3 than or equal to seventeen.

4
5 18. A medium as recited in claim 11, wherein the two input polynomials
6 are representative of integers base R and a length n and wherein $X = R$ in the
7 calculating.

8
9 19. A medium as recited in claim 11, wherein C is zero.
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1
2 **20.** A method comprising:
3 obtaining two input polynomials with six terms each;
4 computing a product polynomial of the input polynomials, wherein the total
5 number of coefficient multiplication operations is fewer than or equal to
6 seventeen;
7 reporting results of the computing.

8
9 **21.** A method as recited in claim 20 further comprising repeating the
10 obtaining and the computing.

11
12 **22.** A method as recited in claim 20 further comprising:
13 selecting a pair of polynomials from a collection of one or more pairs of
14 polynomials and providing the selected polynomials to the obtaining;
15 repeating the selecting, obtaining, and computing.

23. A method as recited in claim 20, wherein during the computing, calculating:

$$\begin{aligned}
& (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
& + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
& + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
& + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - X^3) \\
& + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
& + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
& + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X^2) \\
& + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X^3) \\
& + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
& + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
& + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
& + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
& + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial, where C is a polynomial constant value and the two input polynomials are nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$, respectively.

1 24. A method as recited in claim 23, wherein the variable X is replaced
2 by its negative ($-X$) and the odd-indexed coefficients, $a_1, a_3, a_5, b_1, b_3, b_5$, are
3 replaced by their negatives.

4
5 25. A method as recited in claim 23, wherein the computing is
6 performed in a finite field of characteristic 2, with each even coefficient replaced
7 by zero and each odd coefficient replaced by one.

8
9 26. A method as recited in claim 23, wherein the computing is
10 performed in a finite field of characteristic 3, with each coefficient in claim 4
11 replaced by its modulo 3 image 0, 1 or -1 .

12
13 27. A method as recited in claim 20, wherein the two input polynomials
14 are representative of integers, which are nominally labeled: $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$
15 and $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$, respectively, where $0 \leq a_i < R$ and $0 \leq b_j < R$.

16
17 28. A computer-readable medium having stored thereon a data structure
18 comprising the product polynomial of the two input polynomials, the product
19 polynomial being produced by the method as recited in claim 20.
20
21
22
23
24
25

1
2 **29.** A system facilitating cryptographic security, the system comprising:
3 a memory comprising a set of computer program instructions; and
4 a processor coupled to the memory, the processor being configured to
5 execute the computer program instructions, which comprise:
6 obtaining two input polynomials with six terms each;
7 computing a product polynomial of the input polynomials, wherein
8 the total number of coefficient multiplication operations is fewer than or
9 equal to seventeen;
10 reporting results of the computing.

30. A system as recited in claim 29, wherein during the computing, the computer program instructions further comprise calculating:

$$\begin{aligned}
& (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
& + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
& + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
& + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - X^3) \\
& + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
& + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
& + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X^2) \\
& + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X^3) \\
& + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
& + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
& + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
& + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
& + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
& + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
& + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
& + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
& + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
& + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial, where C is a polynomial constant value and the two input polynomials are nominally described as $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$ and $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$, respectively.

1 31. A system as recited in claim 30, wherein the variable X is replaced
2 by its negative (-X) and the odd-indexed coefficients, $a_1, a_3, a_5, b_1, b_3, b_5$, are
3 replaced by their negatives.

4
5 32. A system as recited in claim 30, wherein the computing is performed
6 in a finite field of characteristic 2, with each even coefficient replaced by zero and
7 each odd coefficient replaced by one.

8
9 33. A system as recited in claim 30, wherein the computing is performed
10 in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its
11 modulo 3 image 0, 1 or -1.

12
13 34. A system as recited in claim 29, wherein the two input polynomials
14 are representative of integers, which are nominally labeled: $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$
15 and $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$, respectively, where $0 \leq a_i < R$ and $0 \leq b_j < R$.

1
2 **35.** A computer-readable medium having computer-executable
3 instructions that, when executed by a computer, performs acts comprising:

4 obtaining two input polynomials each with degree $\leq n$, where n is a positive
5 integer;

6 computing a product polynomial of the input polynomials, wherein the
7 computing has an asymptotic cost is n^c for c with $1 < c < \log(3)/\log(2)$;

8 reporting results of the computing.
9

10 **36.** A computer-readable medium having computer-executable
11 instructions that, when executed by a computer, performs acts comprising:

12 obtaining two input polynomials each with degree $\leq n$, where n is a positive
13 integer;

14 computing a product polynomial of the input polynomials, wherein the
15 computing has an asymptotic cost is n^c for $c = \log(17)/\log(6)$;

16 reporting results of the computing.
17
18
19
20
21
22
23
24
25